

EXHIBIT A

United States District Court

EASTERN

DISTRICT OF

NEW YORK

In the Matter of the Search of

IN THE MATTER OF THE SEARCH OF THE
ELECTRONIC MAIL USER ACCOUNT
matt.tannin@gmail.com

SEARCH WARRANT

CASE NUMBER:

TO: Special Agent John Pinto and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent John Pinto who has reason to believe that ☐ on the person of or ☒ on the premises known as

THE PREMISES KNOWN AND DESCRIBED AS ELECTRONIC MAIL ADDRESS
"matt.tannin@gmail.com"

in the NORTHERN District of CALIFORNIA there is now concealed a certain person or property, namely (describe the person or property) SEE ATTACHMENT A

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before October 19, 2009 Date

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search in the daytime - 6:00 A.M. to 10:00 P.M. and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to any U.S. Magistrate Judge as required by law.

Execution of this Warrant shall be in accordance with Attachment A-I and #19-20 of the Affidavit of Agent Pinto.

October 9, 2009 at 6:37 PM
Date and Time Issued

at Brooklyn, New York
City and State

Hon. Marilyn D. Go
United States Magistrate Judge

Signature of Judicial Officer

TGSW 000000062

Attachment A

I. Service of Warrant and Search Procedure

A. The officer executing this warrant shall effect service by any lawful method to Google.

B. In order to minimize any disruption of computer service to innocent third parties, the officer executing this warrant shall direct Google employees to locate, isolate, and create an exact duplicate of all records and contents of electronic mail associated with the applicable subscriber accounts described in Section II, below, respectively.

C. The term "electronic mail" includes all of the items described in this Attachment in whatever form and by whatever means they may have been created or stored, including without limitation any electronic or magnetic form (such as hard drives, floppy disks, CD-ROMs, backup tapes, and printouts or readouts from any such media), and any handmade, mechanical, or photographic form (such as writing, printing, typing or photocopies).

D. Google employees will provide the exact duplicate in electronic form (or in printouts if the original records are not in electronic form) of the applicable electronic mail messages described in Section II below to the agent who serves this search warrant, who need not be present at the location specified in the warrant during Google's retrieval of records, as permitted in 18 U.S.C. § 2703(g).

II. Electronic Mail and Other Records to be Copied by Google Employees and Seized

All records and other stored information pertaining to the categories specified below, in whatever form kept, in the possession or control of Google, 1600 Amphitheatre Parkway, Building 47, Mountain View, California, 94043, relating to the accounts associated with the Gmail e-mail account "matt.tannin@gmail.com" *from August 13, 2007 through November 7, 2007;*

- i. all subscriber information (including subscriber names, addresses, telephone numbers, dates of birth, social security numbers, account numbers, status of account, duration of account and method of payment);
- ii. all account history (including customer Terms of Service and any complaints);
- iii. all detailed billing records (including date, time, duration, and screen name used each time a particular account was activated);
- iv. a complete log file of all activity relating to the account(s) (including dates, times, method of connection, Internet Provider connection log, port, dial-up and/or location);
- v. all records of subscriber account preferences, including but not limited to, the name and Internet address of any "favorite places" or "book-marked" websites specified by the user(s) of the accounts, along with any "address books," "buddy lists," or "member profiles" maintained by, or related to, the account(s);

- vi. all e-mail from August 13, 2007 through November 7, 2007, including any attachments, and all instant messages, sent by or received by the accounts, whether saved or deleted, whether contained directly in the e-mail account or in a customized "folder"; and
- vii. all web-pages, including any associated links, that were created or maintained by the user(s) of the above-described account from August 13, 2007 through November 7, 2007.

MJF:PT
F.# 2007R01328

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - X

IN THE MATTER OF THE SEARCH OF
ELECTRONIC MAIL USER ACCOUNT
matt.tannin@gmail.com

AFFIDAVIT IN SUPPORT
OF A SEARCH WARRANT

- - - - - X

EASTERN DISTRICT OF NEW YORK, SS:

John Pinto, being duly sworn, deposes and says:

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). As such, I am an "investigative or law enforcement officer" within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516.

2. I have reviewed the attached affidavit in support of a search warrant of FBI Special Agent Mark Munster dated July 7, 2009, attached hereto as Exhibit A, seeking the contents of the SUBJECT E-MAIL ACCOUNT for the period up through August 12, 2007. That search warrant related to the case of United States v. Ralph Cioffi and Matthew Tannin, 08 CR 415 (FB), in which Cioffi and Tannin are charged with conspiracy to commit securities fraud and wire fraud, in violation of 18 U.S.C. § 371; securities fraud, in violation of 15 U.S.C. §§ 78j(b) and 78ff; insider trading (Cioffi only), in violation of 18 U.S.C. §§

TGSW 000000001

78j(b) and 78ff; and wire fraud, in violation of 18 U.S.C. § 1343.

3. This affidavit is submitted in support of a search warrant for the contents of electronic mail ("e-mail") for user account "matt.tannin@gmail.com" ("THE SUBJECT E-MAIL ACCOUNT") on Google, Inc. ("Google"), located at 1600 Amphitheatre Parkway, Building 47, Mountain View, California for the period of August 13, 2007 through November 7, 2007. Based on the facts set forth in this Affidavit, I respectfully submit that there is probable cause to believe that there is presently located in THE SUBJECT E-MAIL ACCOUNT evidence of violations of 18 U.S.C. §§ 371 and 1343, and 15 U.S.C. §§ 78j(b) and 78ff (conspiracy, wire fraud, and securities fraud).

COMPUTERS AND THE INTERNET

4. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I have knowledge of the Internet and how it operates. The Internet is a worldwide computer network which connects computers and allows communications and transfer of information and data across state and national boundaries. Individuals who use the Internet can communicate by using, among other methods, e-mail. The following paragraphs describe some of the functions and features of the Internet as it relates to the subject of this search warrant.

A. Electronic Mail ("E-mail")

5. An e-mail is an electronic communication which usually contains written correspondence and graphic images. It is similar to conventional paper mail (a physical communication) in that it is addressed from one individual to another and is usually considered private.

6. An e-mail usually contains a message "header" which generally displays the sender's e-mail address, the recipient's e-mail address, and the date and time of the e-mail transmission. E-mail addresses on the internet usually appear in a form which contains first the user's name and the name of the Internet service provider, separated by the "@" symbol, e.g., matt.tannin@gmail.com..

B. Google

7. Google offers computer Internet services to its subscribers. One of these services is e-mail, under the domain "@gmail.com". Each Google subscriber uses a computer or wireless device to connect to Google's central computer system operated by Google in northern California. Through e-mail, Google subscribers can send messages to other e-mail subscribers on the internet (whether they are Google subscribers or not) and attach files to those messages. These files (in computer format) may be items such as written documents, or graphic image files which are photographs that have been scanned into the computer system. Both types of files can be printed out by anyone who has "downloaded" them and who has access to a printer.

8. Google subscribers are able to use screen names during communications which in many cases do not provide the subscriber's true name or identifying data. In addition, the subscriber can fill out a subscriber profile which corresponds to the subscriber's screen name. However, the subscriber can put any identifying information into this profile. There is no check by Google or anyone else as to the accuracy of subscriber information entered into this profile.

9. Google maintains records pertaining to its subscribers. These records include subscriber information, account access information, e-mail transactional information, and

other information which records the activities and interactions of these accounts.

10. Any e-mail that is sent to a Google subscriber is electronically stored in the subscriber's "mail box" on Google's central computer system until the subscriber connects to the Google computer system and retrieves his or her messages. After a subscriber retrieves and deletes a particular message, the message will also be deleted from Google's computer system. If, however, a subscriber retrieves a message and does not delete it, the message will remain on Google's computer system.

THE SUBJECT E-MAIL ACCOUNT AND FACTS SUPPORTING PROBABLE CAUSE

11. A copy of the Indictment captioned United States v. Ralph Cioffi and Matthew Tannin, 08 CR 415 (FB), is attached hereto as Exhibit B and incorporated by reference into this Affidavit. There are nine counts in the Indictment, including conspiracy to commit securities fraud and wire fraud, in violation of 18 U.S.C. § 371; securities fraud, in violation of 15 U.S.C. §§ 78j(b) and 78ff; insider trading (Cioffi only), in violation of 18 U.S.C. §§ 78j(b) and 78ff; and wire fraud, in violation of 18 U.S.C. § 1343.

12. In or about November 2007, the U.S. Attorney's Office for the Eastern District of New York and the Securities and Exchange Commission received a paper copy of an e-mail string ("The G-Mail") which was sent from THE SUBJECT E-MAIL ACCOUNT to

the e-mail of "pacioffi@hotmail.com" entitled "Things to Think about - Parts I and II." The first e-mail in the string is date- and time-stamped April 22, 2007 at 8:19 a.m. The second e-mail in the string is from the account of "pacioffi@hotmail.com" to THE SUBJECT E-MAIL ACCOUNT at 10:11 a.m. on April 22, 2007. The third e-mail in the string is from THE SUBJECT E-MAIL ACCOUNT to rmcgarrigal@mac.com at 3:36 p.m. The fourth e-mail in the string is from rmcgarrigal@mac.com to THE SUBJECT E-MAIL ACCOUNT at 4:25 p.m. The content of the e-mail string is excerpted in part in paragraph 41 of the Indictment. The G-Mail was produced by Tannin's counsel to Bear Stearns, which in turn produced it to the U.S. Attorney's Office, and is attached hereto and incorporated by reference into this Affidavit.

13. At or about the same time that Tannin produced The G-Mail, Ray McGarrigal, a former colleague of Tannin at Bear Stearns, produced another, similar paper copy of The G-Mail through his attorney. McGarrigal was interviewed and stated, among other things, that: (a) the account of rmcgarrigal@mac.com was McGarrigal's personal e-mail account; (b) THE SUBJECT E-MAIL ACCOUNT was the personal e-mail account of Matthew Tannin, and (c) the account of pacioffi@hotmail.com was the personal e-mail account of Phyllis Cioffi, wife of Ralph Cioffi. Counsel for Ralph Cioffi represented that, at the time that The G-Mail was sent, he did not have his own personal e-mail account but used

his wife's personal e-mail account. Counsel for Tannin confirmed that THE SUBJECT E-MAIL ACCOUNT was Tannin's personal e-mail account.

14. Based on the investigation of this case, I know that Ralph Cioffi, Matthew Tannin, and Ray McGarrigal all had business e-mail accounts on the Bear Stearns server which they used frequently in the daily course of business. Thus, given the candid nature of The G-Mail, it is likely that Matthew Tannin purposefully used THE SUBJECT E-MAIL ACCOUNT to facilitate the charged conspiracy. The conspirators were able to communicate privately by using THE SUBJECT E-MAIL ACCOUNT, in that their communications would not be subject to capture and review by Bear Stearns.

15. Bear Stearns sent out an evidence preservation notice to its employees, including Tannin, on June 19, 2007. In an interview with counsel for Bear Stearns on June 27, 2007, Tannin was reminded to retain all documents related to the hedge funds he managed. On August 13, 2007, Tannin retained his own counsel in this matter for the first time. On November 14, 2007, an evidence preservation letter was sent to Tannin's counsel by the Securities and Exchange Commission. Tannin's e-mails were subpoenaed by the Securities and Exchange Commission on December 12, 2007. Tannin did not comply with this subpoena. On January 8, 2008, Tannin's counsel agreed to produce to the Securities and

Exchange Commission all e-mails between Tannin and Bear Stearns employees up through and including August 12, 2007. Tannin's counsel has not complied with this agreement.

16. On July 7, 2009 the Honorable Magistrate Judge Cheryl M. Pollak issued a search warrant for the SUBJECT E-MAIL ACCOUNT. Because Tannin first obtained personal counsel on August 13, 2007, the July 7, 2009 search warrant affidavit only requested e-mails through August 12, 2007.

17. Google's initial response to the July 7, 2009 search warrant was that the SUBJECT E-MAIL ACCOUNT had been deleted by Tannin in March 2008, and therefore no responsive material existed. On October 7, 2009, however, Google notified the United States Attorney's Office for the Eastern District of New York that contrary to its earlier representation, Google had in fact retained a copy of the activity, through November 7, 2007, in the SUBJECT E-EMAIL ACCOUNT. On October 8, 2009, Google provided the United States Attorney's Office with the material responsive to the July 7, 2009 search warrant, the e-mails and related material through August 12, 2007.

18. The material that Google provided to the United States Attorney's Office for the Eastern District of New York on October 8, 2009 pursuant to the July 7, 2009 search warrant provides further reason to believe that the SUBJECT E-MAIL ACCOUNT contains evidence of Matthew Tannin's commission of the

charged crimes. In particular, on November 23, 2006, Tannin used the SUBJECT E-MAIL ACCOUNT as a "diary" to write messages to himself. This "diary entry" in the SUBJECT E-MAIL ACCOUNT is attached hereto as Exhibit C and incorporated by reference. In this diary entry, Tannin, among other things, notes that the fund he was running might subject investors to "blow up risk."

19. The government now seeks material from the SUBJECT E-MAIL account from August 13, 2007 through November 7, 2007. Because Tannin engaged private counsel on August 13, 2007, the United States Attorney's Office for the Eastern District of New York will set up a "firewall" and "taint team" procedure to examine the material obtained. In particular, Assistant United States Attorneys who are not part of the Cioffi-Tannin prosecution team (the "walled Assistant US Attorneys") will review all material obtained pursuant to this search warrant in order to determine whether any materials protected by the attorney-client or other privilege are obtained. If the materials are determined not to be privileged, the seized materials will be turned over to the agents and Assistant United States Attorneys prosecuting the Cioffi-Tannin case.

20. If the materials are determined to be privileged, the seized materials will not be shown to the agents and Assistant United States Attorneys prosecuting the case. Any materials that are arguably privileged or in dispute will be

retained by the walled Assistant United States Attorney and submitted to a United States District Court Judge or a United States Magistrate Judge for a ruling as to whether the privilege applies and/or whether the materials fall within any exception to the attorney-client privilege. The arguably privileged materials retained by the walled Assistant United States Attorneys will not be shown to the agents and Assistant United States Attorneys prosecuting the case unless and until a Judge determines that the materials are not privileged or fall within any exception to the attorney-client privilege. In addition, throughout the pendency of this investigation and prosecution, including any appeal, the searching agents will be prohibited from speaking to the Assistant U.S. Attorneys and the agents prosecuting the case about any arguably privileged material unless and until a Judge determines that the materials are not privileges or fall within any exception to the attorney-client privilege.

21. Based on the above, there is probable cause to believe that Matthew Tannin used THE SUBJECT E-MAIL ACCOUNT, and that evidence of the charged crimes is present in THE SUBJECT E-MAIL ACCOUNT.

PARAMETERS OF LEGAL AUTHORITY

22. Title 18, United States Code, Chapter 121, Sections 2701 through 2712, is entitled the "Stored Communications Act" ("SCA"). Section 2703 of the SCA sets forth the procedure that federal and state law enforcement officers must follow to compel disclosure of various categories of stored records from network service providers. As shown from the following provisions of Section 2703, the government may compel disclosure of all stored content and records or other information pertaining to a customer or subscriber of an electronic communication service or remote computer service pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

23. Title 18, United States Code, Section 2703(a) provides, in part:

A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the

contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

24. Title 18, United States Code, Section 2703(b)

provides, in part:

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection -

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service -

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of

providing any services other than storage or computer processing.

25. The government may also obtain records and other information pertaining to a subscriber to or customer of an electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

CONCLUSION

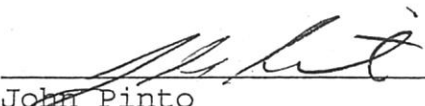
26. Because there is probable cause to believe that Matthew Tannin used THE SUBJECT E-MAIL ACCOUNT in the course of the charged crimes, it is appropriate for the Court to authorize a search warrant of THE SUBJECT E-MAIL ACCOUNT. Contents of THE SUBJECT E-MAIL ACCOUNT are being sought for the period from August 13, 2007 through November 7, 2007. Because Tannin engaged private counsel on August 13, 2007, the United States Attorney's Office for the Eastern District of New York will set up a "wall" and "taint team" procedure to examine the material obtained. In particular, Assistant United States Attorneys who are not part of the Cioffi-Tannin trial team will review all material obtained pursuant to this search warrant in order to determine whether any materials protected by the attorney-client or other privilege are obtained. Such privileged material will not be shared with the Cioffi-Tannin trial team.

27. In addition, I believe that to determine the scope and nature of Matthew Tannin's activity, it is necessary to seize all images, and all text messages, stored in THE SUBJECT E-MAIL ACCOUNT, for the following reasons. First, because voluminous amounts of information can be stored in a computer account, and because it might be stored in a deceptive fashion or with deceptive file names to conceal criminal activity, the searching authorities must carefully open and examine all the stored data to determine which of the various files are evidence, fruits, or instrumentalities of the crime. This sorting process can be extremely time consuming and would be impractical to do at Google's offices. Second, this sorting process must be done in a controlled environment, due to the extensive array of computer hardware and software that might be necessary for computer experts to analyze the data and to recover potentially "hidden," erased, compressed, password-protected, or encrypted files, while at the same time ensuring the integrity of the data recovered and reducing the possibility of inadvertent modification of the data in question.

28. For these reasons, I request authority to seize all images, and all text messages and other content stored in THE SUBJECT E-MAIL ACCOUNT from August 13, 2007 through November 7, 2007, to be searched off-site in a controlled environment. Federal law enforcement officials will review the records sought

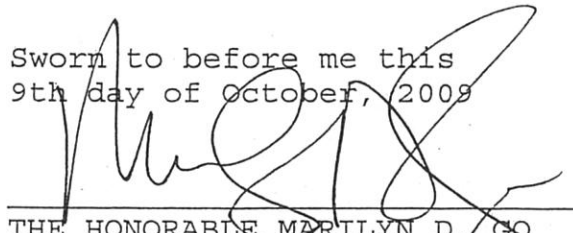
by the search warrant and will segregate any messages and content constituting evidence of violations of federal criminal law.

29. Based on the facts set forth above, I believe there is probable cause to search THE SUBJECT E-MAIL ACCOUNT for evidence of activities relating to conspiracy to commit securities fraud and wire fraud, in violation of 18 U.S.C. § 371; securities fraud, in violation of 15 U.S.C. §§ 78j(b) and 78ff; and wire fraud, in violation of 18 U.S.C. § 1343 and to seize all contents referred to in Attachment A.



John Pinto
Special Agent
Federal Bureau of Investigation

Sworn to before me this
9th day of October, 2009



THE HONORABLE MARILYN D. GO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

Attachment A

List of Items to be Seized

All records and other stored information pertaining to the categories specified below, in whatever form kept, in the possession or control of Google, 1600 Amphitheatre Parkway, Building 47, Mountain View, California, 94043, relating to the accounts associated with the Gmail e-mail account matt.tannin@gmail.com:

for the time period from August 13, 2007 through November 7, 2007:

- (1) all subscriber information (including subscriber names, addresses, telephone numbers, dates of birth, social security numbers, account numbers, status of account, duration of account and method of payment);
- (2) all account history (including customer Terms of Service and any complaints);
- (3) all detailed billing records (including date, time, duration, and screen name used each time a particular account was activated);
- (4) a complete log file of all activity relating to the account(s) (including dates, times, method of connection, Internet Provider connection log, port, dial-up and/or location);
- (5) all records of subscriber account preferences, including but not limited to, the name and Internet address of any "favorite places" or "book-marked" websites specified by the user(s) of the accounts, along with any "address books," "buddy lists," or "member profiles" maintained by, or related to, the account(s);
- (6) all e-mail up from August 13, 2007 through November 7, 2007, including any attachments, and all instant messages, sent by or received by the accounts, whether saved or deleted, whether contained directly in the e-mail account or in a customized "folder"; and
- (7) all web-pages, including any associated links, that were created or maintained by the user(s) of the above-described account up through from August 13, 2007 through November 7, 2007.